

第4章 鉄道分野における安全確保の仕組みと国際規格

中村英夫

信号システムに見るフェイルセーフの思想と規格がもたらす国際競争への影響

ここでは，鉄道の安全を支えている信号システムにおいて，安全のためにどのような仕組みが採用されているのかを解説する．また，鉄道分野における国際規格の動向について解説する．機能安全規格の制定により，鉄道分野においても開発プロセス順守や認証に取り組まないと国際競争力を失いかねない状況になりつつある．この流れは，鉄道という枠を超えて重要な意味を持つものである．　（編集部）

航空機が国を越えて自由に飛行できるように，また，ある国で作られた自動車をほかの国に持って行っても問題なく走らせることができるように，航空機や自動車の技術は国際的な枠組みの中で発展してきました．ところが鉄道は，一つの国の中でも事業者が異なるとシステムが異なり，両方のシステムを搭載しないと走行できない状況にあります．ましてや国が異なると，その独自性も顕著です．

例えば，経済・政治の統合を進める欧州においても，国ごとに異なる鉄道システムが普及していました．そのために欧州連合（EU：European Union）の将来のためには鉄道技術の整合が不可欠の課題とされ，1991年から技術統合に向けての取り組みが開始されています（右掲のコラム「欧州における列車制御システム統合計画」を参照）．

列車輸送の安全を確保する原理や仕組みそのものはそれほど違うわけではないのですが，具体化する段階で多様なシステムが生み出されてきたのです．技術の共用や標準化を求める声も高まりつつあります．国際化の波の中で，既に各国が独自に構築してきた技術にも国際標準を定めようという議論がなされるようになりました．

ここでは，鉄道の安全を支える保安システムを中心に，その安全の仕組みを紹介します．併せて，近年の情報化技術の中で安全性をどのように織り込んできたのか，国際規格策定の流れはどのようなものなのかを，それに対するわが国の取り組みを交えて説明します．

1．「信号システム」で安全を確保する

鉄道の安全には多くの要素が絡み合っています．鉄道は車両，軌道，構造物，電力システムなど多くのシステムから構成されていますが，規模が大きく，しかも広域に展開されています．このため，各構成要素に応じた専門部局が設置され，個々の部局がそれぞれ責任をもって装置やシステムの維持・運用に努めることで，鉄道システムとしての安全が維持されています．

鉄道には，「レールに拘束されて走行する」という特有の条件があります．列車は危険を察知しても，すぐには止まれません．在来線では600m，新幹線では3km近くの距離がかかるのです．そのため，列車同士の衝突や追突といった事故を防ぐには，独特の仕組みが必要となります．そのような保安制御を担当する安全システムを，鉄道では「信号システム」と呼んでいます．その概要を見てみましょう．

● 一つの列車しか走らせない

列車同士の衝突や追突を防止するには，一つの列車しか走らないようにすればよいのです．しかし，線区に一列車では能率が悪いので，線区をいくつかの区間に分割し，そ

KeyWord　信号システム，軌道回路，フェイルセーフ，電子連動装置，IEC 61508，IEC 62278，IEC 62279，RAMS，機能安全，ISO 9000，国際競争

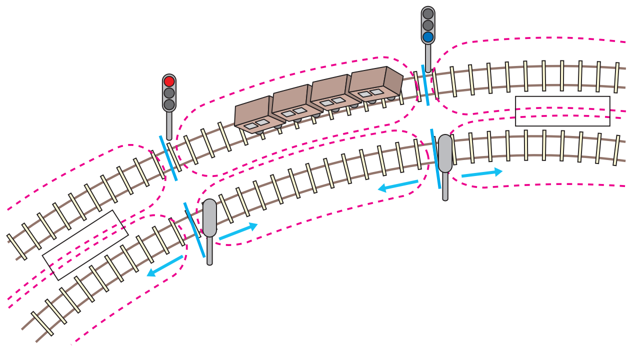


図1　閉塞の仕組み
線区をいくつかの区間に分割し，一つの区間内には一つの列車しか走行できないようにする．この仕組みを閉塞と呼ぶ．閉塞をどのように分割するかは列車の運転能率に関係してくる．首都圏では200mぐらいの間隔に分割しているが，地方では1km以上の間隔で分割した区間もある．

> **COLUMN　欧州における列車制御システム統合計画**
>
> 欧州では，国境を越えて運転される都市間高速鉄道を相互に直通運転できるような鉄道システムの開発を進めています．1986年，欧州経済共同体（EEC：European Economic Community）加盟の12カ国とスイス，オーストリアを加えた14カ国が，21世紀に向けた「ヨーロッパ高速鉄道計画」を定めました．さらに1991年にはヨーロッパ鉄道共同体（the Community of European Railway）を設立し，列車制御技術の共通化を目指した「ヨーロッパ統合列車制御システム（ETCS：the European Train Control System）」の機能とシステム，インターフェース仕様をまとめました．

の区間内には一つの列車しか走行できないようにします（**図1**）．この仕組みを閉塞（へいそく）と呼びます．閉塞区間の入り口には列車が入っているかどうかを表す信号を設備します．列車が入っていれば赤信号にし，後続列車の進入を禁止します．また，赤信号を見ても止まりきれないと困るので，その一つ手前の信号には黄色灯をつけて，次が赤信号であることを伝えます．

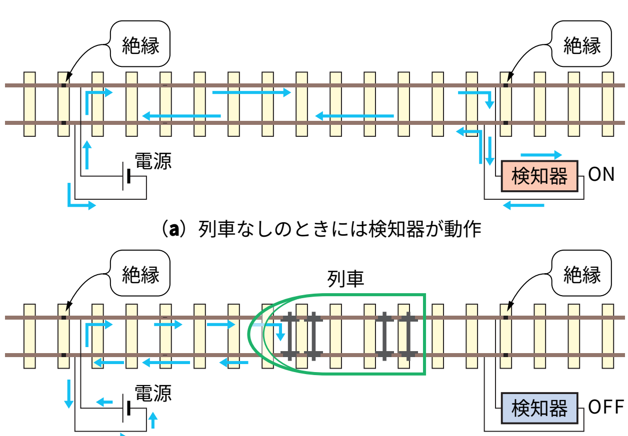
● 列車を検知して安全を守る

列車が閉塞区間に入っているかどうかを知るためには，レールを使った「軌道回路」という仕掛けが使われます．有名なWilliam Robinson氏が今から100年以上も前（1872年）に発明したものですが，いまだに使われています．

軌道回路の仕組みを**図2**に示します．レールを使って受電端の検知器に電流が送られると「列車なし」を検知します（**図2（a）**）．そこに列車が進入すると，2本のレールは車軸によって短絡されます．すると，検知器に送られる電流は減少するので，「列車なし」が検知できません（**図2（b）**）．そこに列車が入っていくことは危険なので，その入り口の信号機を赤にします．

この軌道回路では，停電したり，電線が外れたり，レールが破断したりすると，検知器への電流供給が遮断されます．電流が通電されなければ「列車あり」と同じなので，停止（赤）信号が表示されます．

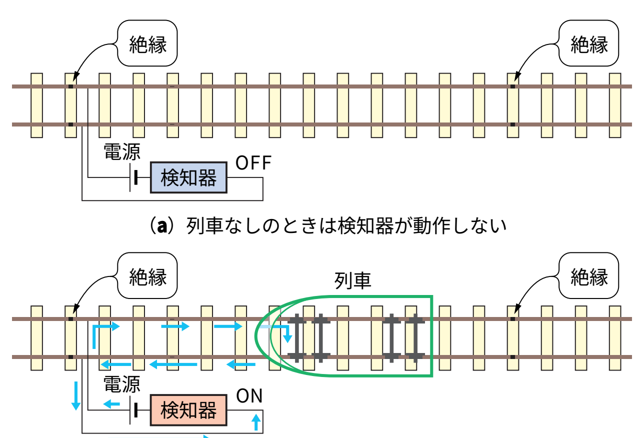
これに対し，**図3**のような回路で列車検知を行ったらどうなるでしょうか．列車がその区間に入れば，車軸を通って通電され，センサが動作するので，この方法でも列車は検知できます．しかし，万一停電していたり，電線が外れ



（a）列車なしのときには検知器が動作

（b）列車が入ると車軸でレールを短絡

図2　フェイルセーフ型の軌道回路
検知器が動作すれば「列車なし」．電源断や配線断のときには「列車あり」になる．



（a）列車なしのときは検知器が動作しない

（b）列車が入ると検知器が動作

図3　非フェイルセーフ型の軌道回路
検知器が動作すれば「列車あり」．電源断や配線断のときには列車が検知できないので，危険な状態になる．

ていたりしたときには，列車の進入を検知できません．このときには，入り口の信号機は進行(青)のままになり，後続列車が閉塞区間に入ることを阻止できないので，危険なことになります．

図2と図3における故障は，信頼性上は同じ「故障」として同一に扱われますが，安全性上は故障時に安全側に動作する(フェイルセーフ)かどうかで区別されます．

● フェイルセーフとともに可用性も確保する

信号システムは鉄道の安全を守る要であり，フェイルセーフの仕組みがあらゆる回路に組み込まれています．例えば，コンデンサは抵抗と対で用いて一定の時間(時素という)を確保したり，異常発振防止に用いられることがあります．しかし，コンデンサのリード線が断線した場合には，時素を確保できない(無時素)とか異常発振を防止できないといった危険側の事態を引き起こします．このため，そのような場所には4端子のコンデンサを用い，断線時には電源供給を断ち，回路は故障となっても無時素や異常発振による危険側の動作を防止する回路にします(図4)．この回路構成もフェイルセーフ技術そのものです(下掲のコラム「今日もまた信号機故障？」を参照)．

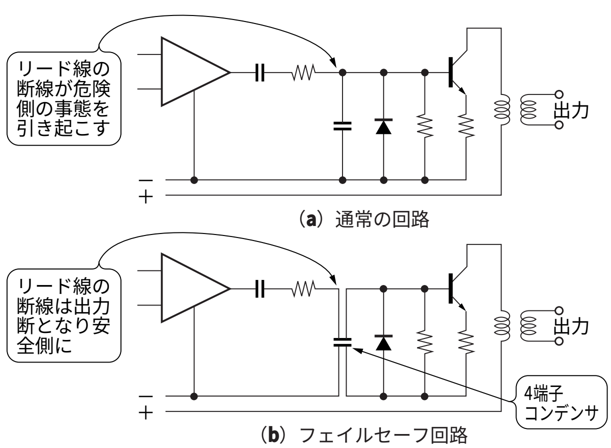


図4　4端子コンデンサを用いたフェイルセーフ回路
4端子コンデンサを用いて，コンデンサのリード線が断線したときは電源供給を断ち，危険側の動作を防止する．

ただ，フェイルセーフとはいえ，故障すると列車を運転できなくなるので，システムとしての可用性の確保も重要です．新幹線の自動列車制御装置(ATC：automatic train control)はこの安全性と可用性の両方を満足させるために，フェイルセーフなシステムを3重系で構成しています．万が一，一つの系が安全側に停止した場合でも，残りの二つの系で運転を継続するように配慮されています．

● 人間のミスを機能で補う

閉塞と信号表示により，衝突や追突を防止する仕組みはそろったわけですが，信号に従わないで運転すると，とんでもない事故が引き起こされます．過去にも三河島事故など，信号機を見誤ったことによる重大事故が多発しました．やはり，運転士の注意力だけに依存していては万全とは言えないのです．このため，運転士が停止信号を見落とすことがないように，停止信号であることを知らせる仕組みを考えました．自動列車停止装置(ATS：automatic train stop)の誕生です．

まず在来線の列車のブレーキ距離を考慮し，停止信号機の手前の地点に，停止信号を伝える装置を設置しました(図5)．この装置が停止信号を伝えると，車上ではブザー音が鳴ります．これに対し，運転士はハンドルをブレーキ位置にして，確認ボタンを押すことになっています(これを「確認扱い」という)．運転士が確認扱いをしないでいると5秒後に非常ブレーキが作動し，列車は停止します．停止信号を伝える地上装置は，ブレーキ距離(600m)に5秒間の走行距離を加えた地点に設置されます．

COLUMN　今日もまた信号機故障？

「信号機のトラブルにより，○×線は上下線とも運転を停止しています」などという交通情報を耳にすることがあります．「今日もまた信号機故障か」と思う方も多いでしょう．しかし，信号機がそんなにしょっちゅう故障しているわけではありません．

列車の運転に信号機の情報は不可欠です．信号機に進行現示(青)が点灯されるには，列車のセンサや転てつ機といった現場の機器はもちろんのこと，連動装置やその上位に位置する進路制御装置などが正常に機能していることが必要です．どこかに故障があるとフェイルセーフに働くので，信号機が停止現示(赤)のままになってしまうのです．

信号機が赤になりっぱなしという状況は，一見信号機そのものが故障したように見えますが，実は奥が深いのです．そして鉄道事業者は，「信号機故障」に結びつくような機器障害が発生しないように，システムの冗長化や保全に力を入れているのです．

このATSは1960年代半ばに全国の国鉄線区に設備され，事故防止に大きく貢献しました．しかし，確認扱いをした後で失念して追突するような事故があったため，今では，さまざまな改良が施されたATSが用いられています．

2005年4月25日に発生した福知山線の列車事故は，乗務員の常軌を逸した運転が原因であるとして問題になりましたが，その事故を受けて，制限速度を超えた運転を防止する機能の追加がATSに求められています．

ATSは人間の運転操作の危険性を事前に検知して安全を守る装置ですが，ブレーキ扱いそのものを機械で自動的に行う自動列車制御装置（ATC）も，新幹線や一部の線区に導入されています．

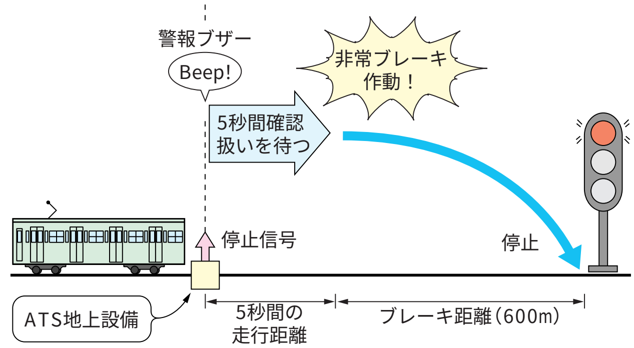


図5　基本的な自動列車停止装置（ATS）の仕組み
停止信号の手前の地点にATS地上設備を設置する．この装置が停止信号を伝えると，運転席でブザー音が鳴る．5秒以内にブレーキ操作と確認扱いをしないと非常ブレーキが作動して，列車は停止信号の手前で停止する．

● フェイルセーフな現場の装置が安全を確保

信号システムには列車の間隔制御のほか，重要な保安制御機能があります．その一つは，単線区間における運転方向の制御です．両駅から列車が出発してしまうと途中で正面衝突してしまうので，両駅の信号機が同時に出発許可を出せないような仕組みが設けられています．これを単線閉塞といいます．

また，駅構内の列車運転の安全確保も重要な機能です．列車ダイヤに従って列車を所定の番線に進行させるためには，その進路中にほかの車両がないこと，ほかの列車が進入してこないことをチェックした上で，進路中にある転てつ機を進路の方向に転換させる必要があります．このような制御と確認を行いながら進路の設定や復位（解除）を行う装置が連動装置です．

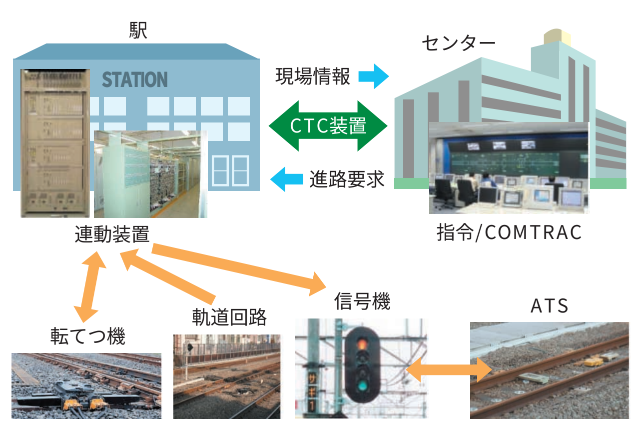
ここまで，閉塞の仕組みや軌道回路，ATS，ATC，連動装置など，信号システムを構成する装置を説明してきました．これらはいずれも現場にある装置（現場機器）であり，フェイルセーフを第一として設計されています（下掲のコラム「中央のコンピュータが安全を守る？」を参照）．例えば連動装置は，さまざまな条件をチェックして進路を

COLUMN　中央のコンピュータが安全を守る？

在来線で列車事故が起きたときなどに，新幹線の安全性と対比する形で「新幹線では中央のコンピュータがすべての列車を管理しているから安全性が高い」といった議論がなされることがあります．確かに，新幹線の運行管理システム（COMTRAC：Computer-aided Traffic Control System）などは，列車の動きをすべて把握しています．しかし，実はそのことと安全性は別問題なのです．

新幹線といえども，列車の安全は軌道回路（列車センサ）とATC，駅構内の連動装置によって保たれています．これらの装置はすべて現場にあり，現場の情報を用いて制御処理を行っています（**図A**）．COMTRACの中央コンピュータは，ダイヤに従って「駅構内の何番線に列車を入れるか」という進路の設定要求を行うだけです．それを受けて，駅の連動装置が進路設定制御を行います．しかも，万一進路を誤った番線に制御してしまったとしても，駅構内の連動装置は，すべての安全条件をチェックして制御された進路を構成するため，安全上は全く問題ありません．もちろん，中央のコンピュータがATCを直接制御するわけでもありません．

このように，安全制御は現場機器で行われています．その点では，在来線も新幹線も差はありません．



図A　現場の信号機器とセンター運行管理システムとの関係
CTC（Centralized Traffic Control）装置を介して指令と現場が接続され，連動装置が核となって現場機器を制御する．

設定しますが，そのチェックはリレー回路によるシーケンス制御で行われてきました．ここで使うリレーは，故障したときには0側に誤るという，特殊な信号用のリレーです．万が一回路に故障が発生しても，必ず赤信号になるように設計されているのです．

2. コンピュータ技術の導入

ところが，この分野にコンピュータ技術が導入されるようになりました．コンピュータの故障モードはさまざまです．これまでの信号機器と同じようにフェイルセーフにするには，すべての故障モードに対して安全側に動作するようにコンピュータを構成する必要があります．

また，コンピュータはソフトウェアによって制御するわけですが，ソフトウェアにはバグがつきものです．コンピュータをフェイルセーフに作れたとしても，ソフトウェアに誤りがあれば致命的です．いかにしてバグのないソフトウェアを作るのか？ あるいはソフトウェアの誤りが危険側に至らないようにするのか? これらを解決しないことには，コンピュータ制御は実用化できません．

● フェイルセーフな電子連動装置の登場

コンピュータの故障に対する対策としては，回路素子を多重系にし，処理結果を照合することにより診断する方法が採られました．故障が検出されたら，いち早く安全側にシステムを遷移させることで，故障に対応できます．

1985年，わが国の鉄道にフェイルセーフなコンピュータ・システムである電子連動装置が登場し，駅構内の信号機器を制御しました（図6）．電子連動装置は3重系構成を採っており，三つのCPUの信号線をマシン・サイクルごとに比較照合することで，故障を診断していました．

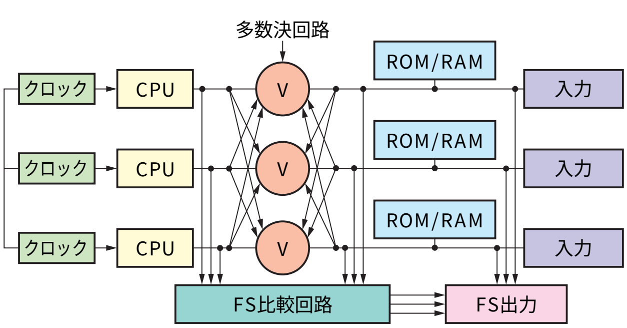


図6　電子連動装置SMILEのハードウェア構成
三つのCPUの信号線をマシン・サイクルごとに比較し，その値をバスに挿入された多数決回路により訂正して使用する．

● ソフトウェアはシングル・スレッドで安全を確保

組み込みシステムは，リアルタイムOSのもとでさまざまな状況の変化に応じて処理できるように，マルチタスク構成を採るものが少なくありません．外部イベントの変化を割り込みとして利用し，最優先されるタスクに切り替えてリアルタイム性を確保します．これに対し，電子連動装置のソフトウェアは，割り込みに応じてタスクを切り替えるのではなく，それぞれの処理を数珠つなぎにして，次々とシーケンシャルに実行する「シングル・スレッド方式」で動作しています．

マルチタスク構成は確かにリアルタイムOSの神髄で，高機能な組み込みシステムになくてはならないものです．一方で，タスクが複雑に切り替わることで思いがけないバグを誘発しかねないことも事実です．シングル・スレッド方式では各タスクの動き方が一義に定まっているので，クリティカルなタスクの切り替えタイミングで発生するバグも回避できるし，タスクの誤った動きを検出するのも容易です．

そのほか，ソフトウェアを以下のような仕様として，安全性に配慮しています．

1）割り込みを使わない

タスクの動作中には，割り込みを受け付けません．一連の処理の最終タスク（スレッドの終わりのタスク）が終わってほかのスレッドの先頭タスクに戻る際に，割り込み要因を分析し，次のスレッドにおいて，対応する処理を行います．

2）周期的に処理を行う

イベントの発生に応じて必要な処理を行うのではなく，シングル・スレッドで繰り返し処理するので，同じ処理が周期的に行われることになります．従って，出力データが常にリフレッシュされることになり，出力ポートの値が万が一ノイズなどによって書き換わっても，次のサイクルで訂正されることになります．

3）タスク間通信で危険側の情報を厳重に検査する

タスク間で処理データを交換するとき，危険側に遷移させるような制御につながる情報であれば，受け入れ検査を厳重に行います．安全側に遷移させるような情報であればそのまま使用します．

4）危険側の入力変化を診断する

入力値の変化をそのまま受け入れるのでなく，安全性に配慮した処理が組み込まれています．例として，線路上に列車が存在するかどうかについての情報（在線情報）を考えます．入力値が「列車あり」に変化した場合は，停止信号につながる処理が行われるので安全側です．従って，この変化は素直に受け入れます．入力値が「列車なし」に変化した場合は，「同じ情報が何回も入力されるか」といったチェックをしてから使うことで，万全を期します．

5）入力変化の合理性を診断する

入力値の変化に対しては，4）のような非対称診断とは別に，「そのような変化があり得るものかどうか」を診断した上で使うように配慮しています．例えば，列車の動きをトレースし，入力情報の変化について合理性を診断します．

このような合理性診断は，リレー・シーケンス制御の時代には困難でした．かつて，レールが汚れていて列車が検知できなかったため，「その区間には列車が存在しない」と認識されて事故を引き起こしたこともありました．しかし，列車を追跡していれば，ここで列車が消えるはずがないということが分かるので，その情報を誤りとすることができます．これなどは，コンピュータの情報処理機能を利用することで実現した処理であると言えます．

このように，安全性を確保するために独特な手法が組み込まれました．また，連動機能は駅の構内配線に応じて変わります．基本戦略として処理プログラムは各駅共通とし，異なる配線条件などはデータとして与える構造にする方式が採られました．

また，一般的な高信頼化手法も採用されました．バグそのものの発生確率を低くするため，メーカの中には「各プログラム・モジュール（タスク）を100行以下とする」といった基準や，使用するコンパイラに制限を付けるなどといった自主規定をもって臨むところもありました．

● 安全性確保の手引きと国際規格

信号システムへのコンピュータ導入は，スムーズに進んだわけではありません．既存のリレー・シーケンスによる機器と同等以上の安全性を立証することが必須の要件でした．そのために，鉄道総合技術研究所は，鉄道信号のマイクロエレクトロニクス化の開発のよりどころとなる指針を1983年の段階で作成し，コンピュータを用いたシステムにおける安全性確保に対する考え方を明確にしました（図7）．



図7　信号保安装置へのマイクロエレクトロニクス導入指針
既存のフェイルセーフ技術を，コンピュータ技術に置換するためのよりどころとして利用された．

さらに，その妥当性を立証するために，徹底したフィールド試験を実施しました．電子連動装置の実用1号機は1985年3月に東神奈川駅で実制御を開始しましたが，その後，電子閉塞装置，電子踏切装置，新幹線ATC車上装置というように，次々とコンピュータ制御式の信号装置が開発されます．

3．ソフトウェア・システムの安全技術指針と国際規格

電子連動装置や電子閉塞装置の開発で生み出された各種の安全性技術はデータベース化され，安全性の指針とともに，以後の技術開発でも積極的に利用されました．このような技術開発の流れの中で，鉄道総合研究所は，ソフトウェアを使った安全関連制御機器に関する規格を策定しようという国際的な動向に早くから着目していました．そして，1994年の段階で委員会を組織し，国際規格IEC 1508（現IEC 61508）の審議の動向を踏まえ，その規格の精神を先取りした「安全性技術指針」の検討を開始しました．これは，電子連動装置の実用化から10年を経て蓄積された安全性技術をもとに，これからの保安制御システム開発に利用できる指針を作成しようとしたものです．

委員会は1995年に「列車保安制御システムの安全性技術指針」を作成しました．その技術指針は審議中の国際規格の精神に沿う形で作成されました．すなわち，事前安全性解析の段階でシステムのリスク解析を実施することや，達成するべき安全度水準（SIL：safety integrity level），実

現するべき保安機能などを明確にすることを求めています．また，各製造プロセスにおいて厳格に安全性を織り込む点でも，規格の精神を踏襲しています．鉄道信号の世界に「リスク」という概念が初めて登場したのも，この技術指針でした．

ところで，この技術指針やIEC 61508の思想にのっとってシステム開発を行うと，これまで行われてきた開発作業に加えて，審査や文書（ドキュメント）整備などの作業が必要になります．このため，製造コストの増加につながるとか，指針の中で利用可能な安全性技術を公開することは，企業のノウハウをオープンにすることになり好ましくないといった否定的な意見も多数ありました．

一方で，この指針の意図を積極的にとらえ，新しい電子連動装置の開発に際し，要求されるプロセスに準拠して実践してみようという試みも行われました．その結果は学会論文として発表されましたが，「厳格なプロセスの実行により，バグ件数の削減や収束の速さから結局生産性も向上した」との見解が披露されています．

● IEC 61508の制定と鉄道用規格

鉄道に限らず，安全はさまざまな産業領域においても重要な課題です．それぞれの産業領域で，安全を守るためのフェイルセーフ技術が生み出されてきました．しかし，フェイルセーフ技術を議論し，共通の土壌を形成しようとしても，議論がかみ合わないという状況が続きました．

例えば鉄道では，機器や回路に「たとえ故障しても安全側に動作する」ように構成することをフェイルセーフとして，そのための技術を構築してきています．一方，航空機では，機器や装置の故障によって機能が停止すると飛行を継続できないので，何とかして機能を維持しようとする技術をフェイルセーフとしてきています．このように定義が異なっている領域間で，技術上の接点を求めるのが容易でないことは明らかです．

しかし，リスクという尺度を用い，そのリスクを軽減するための努力という視点でとらえると，あらゆる産業界の安全性向上のための営みが同一となります．しかも，コンピュータ制御という共通の技術が普及することにより，リスク軽減のための技術も共通に議論できるようになりました．

このような状況を背景として，機能安全規格「IEC 61508」が2000年に制定されました．IEC 61508は産業界に共通の汎用規格であり，この規格をもとに個別分野の規格が展開されることを想定しています．鉄道分野では，欧州規格（European Standard）をベースに審議した結果，2002年にIEC 62278とIEC 62279が制定されました（**表1**）．

IEC 62278は，信頼性（reliability），可用性（availability），保守性（maintainability），安全性（safety）を確保するための実施事項を規定しています．これらの頭文字をとって「RAMS（ラムズ）の規格」とも呼ばれています．また，ソフトウェアに関する規格は，IEC 62279という別の規格として制定されました．

なお，EN 50129は，安全度水準の決定方法について言及しています．一般的なリスク低減プロセスとして，開発時のリスク解析によるリスクの水準と許容できるリスク水準，安全性技術を導入した後の残存リスクの関係は**図8**のように表現できます．安全度水準は，現存（リスク解析時）のリスク水準と許容できるリスク水準のギャップの大きさによって決まるとされています．また，定めようがない場合の参考事例として，許容できる失敗確率（THR：tolerable hazard rate）に基づいてSILを決定する方法が示されています[注1]．

注1：許容できる失敗確率とSILの対応を示した表は，IEC 61508で規定されている目標機能失敗尺度（連続モード運用の場合）と同じものである．目標機能失敗尺度については，本特集第1章の表2を参照のこと．

表1 鉄道分野における機能安全の国際規格

規格番号	表　題	ベースとなった欧州規格	概　要
IEC 62278（2002年に策定）	Railway Applications - Specification and demonstration of reliability, availability maintainability and safety（RAMS）	EN 50126	機能安全規格「IEC 61508」の鉄道分野向けのサブ規格
IEC 62279（2002年に策定）	Railway Applications - Communications, signalling and processing systems - Software for railway control and protection systems	EN 50128	IEC 62278と同時に策定された，ソフトウェアに関する規格
IEC 62425（審議中）	Railway Applications - Safety related electronic systems for signalling（safety case）	EN 50129（1998年に策定）	信号システムの認証と受け入れに必要な安全性要件と，その文書管理について述べた規格

● 国際規格適用のケース・スタディからの見解

筆者はケース・スタディとして，RAMSの規格の作業フローに従って安全性評価を実施してみたことがあります．対象とした装置は，安全上重要(バイタル)な処理機構と，パソコンで行うノンバイタルな処理部から構成されるものでした．評価作業は委員会形式で行われましたが，その際にもリスク解析には多くの議論がありました．

これまで，鉄道の信号システムではフェイルセーフを絶対として，事前安全性解析で抽出された致命的事象に対し，フェイルセーフのための対策を漏れなく網羅的に実施するという立場を取ってきました．もちろん，その結果としてどのくらい危険側故障率が残留しているのかについても評価していましたが，あくまでも念のためであり，評価手法も厳密なものではありませんでした．そのため，時間をかけてリスクを算出する必要性を感じないという意見が少なからずありました．

また，リスクの頻度を求めるデータが不足していること，作業に多くの仮定を伴うことなども，リスク解析を疑問視する理由となりました．リスク解析の目的はシステムの安全度水準(SIL)を定めることにあります．「SILのレベルに応じて製造工程の各プロセスにおける作業の内容を規定し，結果として要求される安全性を達成する」．これが一連の機能安全規格の基本思想であり，SILは重要な意味を持ちます．とはいえ，SILはたかだか4段階のものであり，詳細に計算した結果によらなくても，そのシステムの使命と危険性を考えれば，システムにSILを割り当てることは十分可能です．例えば，「ATCは絶対に安全でなければならないのでSIL4．自動運転はATCの下で機能するので，安全上は制約が緩く，SIL3で十分だろう」などです．この直感による値が詳細なリスク解析による結果と異なることはあり得ないし，もし異なったとしても，果たして，十分とは言えないデータの積み上げによる数値の方が意味を持つと断言できるかどうか分かりません(下掲のコラム「リスク解析は安全対策のため？ SILを割り当てるため？」を参照)．

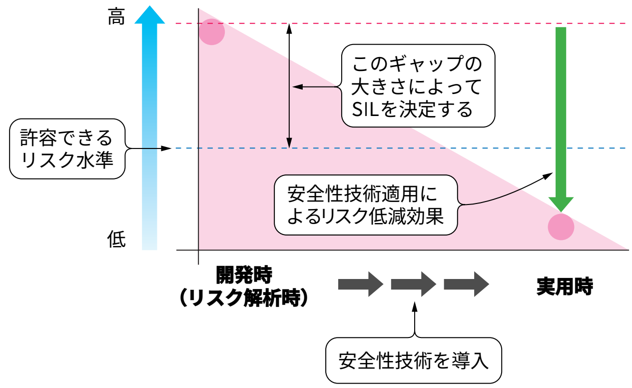


図8　リスク解析と安全度水準(SIL)との関係

開発対象が持つリスクを，許容できる水準まで低減させるために，安全性技術が用いられる．その隔たりが大きければ大きいほど，より安全度水準の高い技術が必要になる．

このように，わが国はこれまで機能安全規格を積極的に利用してきたとは言えません．しかし今後は，欧州での動向を受け，機能安全規格を無視できない状況になるものと思われます．しかも，認証機関の介在により，数量的評価の要求が強まる懸念もあります．規格の本来の趣旨は，各プロセスの作業を厳格に行うことにより，安全関連装置の

COLUMN　リスク解析は安全対策のため？ SILを割り当てるため？

IEC 61508やその関連規格ではリスク解析を重要視していますが，このリスク解析の位置付けを明確にする必要があるでしょう．安全性工学の分野では，原子力産業などで行われている「確率論的安全設計」と，鉄道などのように，フェイルセーフを第一としてあらゆる故障に対し本質的に安全であることを求める「決定論的安全設計」を分けて考えます．このうち，確率論的安全設計の基本となるのが，リスク解析です．

確率論的安全設計は，考え得るすべての傷害要因を列挙し，その影響をリスクとして評価して，その値が許容できるレベルになるまで対策を施します．網羅的に，ささいな因子でもすべて抽出し，それぞれに対してリスクを評価することの重要性と有効性は，これまでの原子力産業界などにおける実績が物語っています．

一方，近年国際規格などで用いられているリスク解析は，システムの安全度水準(SIL)を得るための手段としての色彩が強く，確率論的安全設計とは(同一の尺度を用いてはいるものの)目的とするところは異なっているように思います．このことを抜きにして，SILを得るために詳細にリスク解析を実施しても，少なくともシステムのイメージが明確に把握できるような対象に適用する限りでは，無駄が多いと言えます．

開発の初期段階(事前安全性解析)でリスクを詳細に算出するよりも，個々のコンポーネント(ハードウェア/ソフトウェア)にSILが与えられた後，SILに応じた安全性ライフ・サイクル・プロセスの順守事項を厳密に実行することの方が重要ですし，本来の規格の趣旨であったはずです．

安全性を向上させることです．評価のための評価になることのないよう，留意する必要があると思います．

● ソフトウェアの安全性と国際規格

製品に組み込まれるソフトウェアの安全性確保と流通を考えたとき，IEC 61508に代表される規格の方法論は合理的であり，ほかに取って代わり得る方法はないとも思われます（下掲のコラム「開発プロセスを規定するIEC 61508は調達側に朗報」を参照）．しかし，セーフティ・クリティカル・システム用のソフトウェアに関する規格という視点で眺めると，まだまだ不足な点も実感されます．その主なポイントを以下に示します．

1）ソフトウェアへのSILの割り当て方法が不明確

システムのSILが算出された後に，ソフトウェアにどのようにしてSILを割り当てるかの方法論がまだあいまいと言えます．

2）ソフトウェア・モジュールへのSILの割り当て方法が不明確

システムに組み込まれるソフトウェア・モジュールにも，安全性へのかかわり具合には差があります．ソフトウェア（モジュール）の独立性に対する吟味を踏まえた上で，個々のモジュールに対するSILの割り当て方法を明確にする必要があります．

3）過去の経験に学ぶサイクルが確立されていない

ソフトウェアに限るものではありませんが，安全性手法の多くは，過去の事故を教訓として確立してきています．過去にソフトウェアが引き起こした事故を見ても，そこから学ぶべきことは数多くあります．IEC 61508には，このような事例に学びつつ発展させていくという視点や方法論が不足しています．

4）システムとしての安全性を網羅しきれていない

システムの安全を確保するには，物を作るとき（開発）だけでなく，運用や保全といったヒューマン・ファクタにかかわることも重要です．IEC 61508は「計画から廃棄に至るまでの全ライフ・サイクルを通じた規格である」との建前をとっていますが，実態は，物作りの規格にとどまっているように思われます．

5）SIL算出に用いる具体的なデータが不足している

安全度水準（SIL）を重要な尺度としているものの，その根拠となる発生頻度などの算出に用いるための具体的なデータが不足しています．

4．規格がもたらす国際競争への影響

IEC 61508などの国際規格がソフトウェアの安全性に対して果たす役割は，もちろん肯定的に評価されるものです．ただ，規格がもたらすもう一つの側面についても触れておかないと，禍根を残すことになるかもしれません．それは産業界における国際競争という面で見たときの，規格の果たす役割です．

つまり，「国際規格にのっとっていることが認証された製品」の購入を排除することが困難であると同様に，「国際規格にのっとっていることが認証されていない製品」の購入排除が合法的に可能である，ということです．この原則の下で国際競争が行われたとき，わが国の産業界にどのような影響があるかは大きな問題です．

● 国際規格認証品と日本の物作り

わが国の物作りは，出来上がった「物」で勝負するという文化が支配していました．かつての電子機器がそうでした

COLUMN　開発プロセスを規定するIEC 61508は調達側に朗報

IEC 61508は安全関連システムのソフトウェア開発のプロセスを規定していますが，これは製造面に効果をもたらすのみならず，実は，安全関連システムを調達する側にとっても意義のあることです．これまで，機能仕様に従って作られたソフトウェアの良しあしをどのようにして評価するのかは，調達側にとって厄介な問題でした．安全にかかわる問題だけに，複数の製品をコストのみで評価してよいはずがありません．

調達後に万が一事故が発生した場合には，誰が責任を取ればよいのでしょうか．安全にかかわるソフトウェアですから，可能な範囲の事前検査で潜在バグが顕在化するほど品質は低くないはずです．とするなら，購入を決定した調達者の責任を問うこともできなそうです．

このような問題に対し，IEC 61508の世界では，どのような作り方をしたのか，またその作り方は妥当であるかどうかが第三者によって評価されます．そのため，その結果をもとにして，調達側で評価することもできるでしょう．審査やプロセスが形骸化していたなら，それは製造側と認証者の責任とすればよいので，それについて調達側で悩む必要はなくなります．

COLUMN 安全への投資

ATSやATCなどといった，人間のミスによる事故を未然に防ぐための装置（機械化の仕組み）が，安全性の向上に大きく貢献してきました．しかし，機械化にも限界があります．設計や工事実施といった業務はまだまだ人間に依存せねばならず，その領域でのミスによる事故も絶えません．

JR東日本は，人間と人間の注意力に依存して行われる現場工事や現場作業に情報技術を導入することで，事故防止を図る取り組みを進めています．作業の許可や終了入力と列車の運転をリンクさせたり，作業員に自ら列車の進路を要求させたりすることで，ヒューマン・エラーに起因する事故を減少させようとしています．

このような取り組みを含め，安全施策を推進するには多大な資金が必要となります．JR東日本の2006年度の設備投資計画によると，安全対策に前年度より3割（約340億円）増の1490億円が投資されるといいます．同年度の設備投資の総額は3300億円ですから，安全対策に5割近くを投資することになります．羽越線の突風による事故やJR西日本福知山線の事故を踏まえ，さらなる安全性向上を図ろうという取り組みです．

し，今日の自動車産業も，製品に対するユーザの信頼が競争力を支えている点では同じでしょう．使ってもらって，その信頼性や機能性の素晴らしさを実感してもらえればおのずと勝負がつく，という考え方です．金型や微細加工といった技術は日本の伝統産業とも言えるもので他国を圧倒していますが，決して形式化された製造プロセスや，ドキュメントの素晴らしさが基本にあるわけではありません．

コンピュータを用いた信号装置も同様で，プロセスよりも実体が重視されてきました．コンピュータ式信号装置の開発には，発注側の技術者と製造者の技術者が共同で参画し，徹底した議論と検証を積み重ねてきました．従って，その製品がどのようなものであり，安全性もどのようなレベルであるかは，双方とも熟知していましたし，責任も持ち得ていました．

しかし，国際規格が描く物作りの世界は，「製造プロセスの妥当性と，その認証をもって評価しよう」という，全く異質なものです．そのフレームの原型は，品質保証に関する規格「ISO 9000」に見ることができます．

● ISO 9000を戒めとせよ

かつて，わが国の工業製品は圧倒的な品質の良さで世界をしのいでいました．価格が少々高くてもわが国の製造刻印がある製品は売れる，という事態も起こり，やがてそれが貿易摩擦を引き起こす要因にもなりました．そのような高品質の製品を生み出した背景には，QC（quality control）やTQC（total quality control）という製造現場での品質管理運動が有効に機能していたことが挙げられます．優秀な労働力と安定した雇用に支えられた現場からの品質改善運動は，契約社会の欧米はもちろん，他国ではなかなかまねができず，垂ぜんの的ともなっていました．

しかし，ISO 9000がこの枠組みを津波のように崩壊させました．ISO 9000の世界では，優れた品質の証しを製造プロセスの水準に求めることになったのです．すなわち，「品質が保証された製品を製造するために生産現場で求められるプロセス」を規定し，「そのプロセスで製造されている証し（evidence）と第三者による認証を品質保証のよりどころとする」，という枠組みを作り上げたのです．ISO 9000を取得している工場からの製品を拒むことは貿易障壁と見なされるし，取得していない工場からの製品は，たとえ良品であっても排除できるのです．

わが国の製造業界は，こぞってISO 9000の資格認証に動き出し，従来のTQCはいつの間にか現場から姿を消しました．リコールが相次ぐわが国の現状を見れば，事の重大さが分かると思います．

しかも，製品安全に対する認証機関やその仕組みは，欧米では産業として成り立つほど成熟しています．わが国が明確な戦略を持たずに国際規格時代に突入することは，あまりにもリスクが大きすぎます．この事実をしっかり認識するべきでしょう．

なかむら・ひでお
日本大学 理工学部 電子情報工学科

<筆者プロフィール>
中村英夫．1948年生まれ．鉄道総合技術研究所で信号保安装置，列車制御装置のコンピュータ化やシステム化に長年従事．研究領域は鉄道のほかシステム安全工学，システム工学など多岐にわたる．酒の肴と美酒を前にしての語らいは拒むことなし．日本信頼性学会前会長．現在日本大学教授．東京理科大卒，工学博士．

4